

# Matching subspaces in a field extension: an update

Shalom Eliahou\* and Cédric Lecouvey†  
 LMPA Joseph Liouville, FR CNRS 2956  
 ULCO, B.P. 699, F-62228 Calais cedex  
 Univ Lille Nord de France, F-59000 Lille, France

## Abstract

In this paper, we formulate and prove linear analogues of results concerning matchings in groups. A matching in a group  $G$  is a bijection  $\varphi$  between two finite subsets  $A, B$  of  $G$  with the property, motivated by old questions on symmetric tensors, that  $a\varphi(a) \notin A$  for all  $a \in A$ . Necessary and sufficient conditions on  $G$ , ensuring the existence of matchings under appropriate hypotheses, are known. Here we consider a similar question in a linear setting. Given a skew field extension  $K \subset L$ , where  $K$  commutative and central in  $L$ , we introduce analogous notions of matchings between finite-dimensional  $K$ -subspaces  $A, B$  of  $L$ , and obtain existence criteria similar to those in the group setting. Our tools mix additive number theory, combinatorics and algebra. The present version corrects a slight gap in the statement of Theorem 2.6 of the published version of this paper.

**Keywords.** Linear Matchings; Additive combinatorics; Systems of distinct representatives; Hall theorem; Matroids; Free transversals.

## 1 Introduction

Throughout the paper, we shall say *field* for a skew field or division ring, and *commutative field* for a field in which the product is commutative.

---

\*eliahou@lmpa.univ-littoral.fr

†lecouvey@lmpa.univ-littoral.fr

Let  $G$  be a group, written multiplicatively. Let  $A, B \subset G$  be nonempty finite subsets of  $G$ . A *matching* from  $A$  to  $B$  is a map  $\varphi : A \rightarrow B$  which is bijective and satisfies the condition

$$a\varphi(a) \notin A$$

for all  $a \in A$ . This notion was introduced in [6] by Fan and Losonczy, who used matchings in  $\mathbb{Z}^n$  as a tool for studying an old problem of Wakeford concerning canonical forms for symmetric tensors [19]. Obvious necessary conditions for the existence of a matching from  $A$  to  $B$  are  $|A| = |B|$  and  $1 \notin B$ . The group  $G$  is said to have the *matching property* if these conditions on  $A, B$  suffice to guarantee the existence of a matching from  $A$  to  $B$ . What groups possess the matching property, and when are there automatchings from  $B$  to  $B$ ? The following answers were first obtained by Losonczy [12] in the abelian case, and then extended to arbitrary groups in [3].

**Theorem 1.1** *Let  $G$  be group. Then  $G$  has the matching property if and only if  $G$  is torsion-free or cyclic of prime order.*

**Theorem 1.2** *Let  $G$  be a group. Let  $B$  be a nonempty finite subset of  $G$ . Then there is a matching from  $B$  to  $B$  if and only if  $1 \notin B$ .*

Theorem 1.1 and 1.2 were established using methods and tools pertaining to additive number theory and combinatorics. Specifically, the additive tools used are lower bounds on the size of the product set

$$AB = \{ab \mid a \in A, b \in B\}$$

in  $G$ , and the main combinatorial tool is Hall's marriage theorem. See also [8] for more results on matchings in groups.

Now, various additive theorems bounding  $|AB|$  have recently been transposed to a linear setting, in the following sense. Given a field extension  $K \subset L$  and finite-dimensional  $K$ -subspaces  $A, B$  of  $L$ , analogous lower bounds on the dimension of  $\langle AB \rangle$  were established, where  $\langle AB \rangle$  is the  $K$ -subspace spanned by the product set  $AB$  in  $L$ . See [10, 9, 4, 5]. Suitable hypotheses on the extension may be needed, such as commutativity or separability. Two main results in [4], which play a key role here, only require  $K$  to be commutative and central in  $L$ .

The purpose of this paper is to show that Theorem 1.1 and 1.2 also admit linear analogues in a field extension  $K \subset L$ . As in [4], we only assume that  $K$  is commutative and central in  $L$ . In Section 2, we introduce a specific notion of matching bases of finite-dimensional subspaces  $A, B$  of  $L$ , and state the main results of the paper, namely Theorem 2.6 and 2.8. They are analogous to Theorem 1.1 and 1.2, and give existence criteria for such matchings. The possibility of matching a given basis of  $A$  to some basis of  $B$  is reformulated in Section 3, in terms of suitable dimension estimates. In the process, we use a linear version of Hall's marriage theorem, derived from a more general theorem of Rado on the existence of independent transversals in matroids. Section 4 presents the linear versions in [4] of results in additive number theory, that will allow us to deal with the required dimension estimates of the preceding section. This is achieved in Section 5, where Theorem 2.6 and 2.8 are finally proved. In the last section, we introduce and study a related notion of strong matching between subspaces of  $L$ .

## 2 Definitions and main results

Throughout the paper, we shall consider a field extension  $K \subset L$ , where  $K$  is commutative and *central* in  $L$ , i.e. such that  $\lambda x = x\lambda$  for all  $\lambda \in K, x \in L$ . Let  $A, B \subset L$  be finite-dimensional  $K$ -subspaces of  $L$ . Ideally, a matching from  $A$  to  $B$  would be an isomorphism  $\varphi : A \rightarrow B$  such that  $a\varphi(a) \notin A$  for all non-zero  $a \in A$ . However, we need to introduce somewhat subtler requirements in order to obtain existence criteria analogous to those of Theorem 1.1 and 1.2.

To start with, observe that if  $0 \neq a \in A$  and  $b \in B$ , then

$$ab \notin A \iff b \notin a^{-1}A \cap B.$$

This motivates the use of the subspace  $a^{-1}A \cap B$  of  $B$  in the definition of matched bases below.

**Definition 2.1** *Let  $A, B$  be  $n$ -dimensional  $K$ -subspaces of the field extension  $L$ . Let  $\mathcal{A} = \{a_1, \dots, a_n\}$ ,  $\mathcal{B} = \{b_1, \dots, b_n\}$  be bases of  $A, B$  respectively. We say that  $\mathcal{A}$  is matched to  $\mathcal{B}$  if*

$$a_i b \in A \implies b \in \langle b_1, \dots, \widehat{b_i}, \dots, b_n \rangle$$

for all  $b \in B$  and all  $i = 1, \dots, n$ , where  $\langle b_1, \dots, \widehat{b_i}, \dots, b_n \rangle$  is the hyperplane of  $B$  spanned by the set  $\mathcal{B} \setminus \{b_i\}$ ; equivalently, if

$$a_i^{-1}A \cap B \subset \langle b_1, \dots, \widehat{b_i}, \dots, b_n \rangle \quad (1)$$

for all  $i = 1, \dots, n$ .

**Remark 2.2** If  $\mathcal{A}$  is matched to  $\mathcal{B}$  in the above sense, then it follows that

$$a_i b_i \notin A,$$

and hence  $a_i b_i \notin \mathcal{A}$ , for all  $i = 1, \dots, n$ . In particular, the map  $a_i \mapsto b_i$  is a matching, in the group setting sense, from  $\mathcal{A}$  to  $\mathcal{B}$  within the multiplicative group  $L^*$ .

Moreover, we now show that if  $\mathcal{A}$  is matched to  $\mathcal{B}$ , then  $B$  cannot contain 1. This necessary condition exactly mirrors the corresponding one in the group setting.

**Lemma 2.3** Let  $A, B$  be  $n$ -dimensional  $K$ -subspaces of the field extension  $L$ . If a basis  $\mathcal{A}$  of  $A$  can be matched to a basis  $\mathcal{B}$  of  $B$ , then  $1 \notin B$ .

**Proof.** Let  $\mathcal{A} = \{a_1, \dots, a_n\}$ ,  $\mathcal{B} = \{b_1, \dots, b_n\}$  be bases of  $A, B$  respectively. Assume on the contrary that  $1 \in B$ . Then we have

$$1 \in \bigcap_{i=1}^n (a_i^{-1}A \cap B).$$

On the other hand, it is clear that

$$\bigcap_{i=1}^n \langle b_1, \dots, \widehat{b_i}, \dots, b_n \rangle = \{0\}.$$

Therefore, the inclusion  $a_i^{-1}A \cap B \subset \langle b_1, \dots, \widehat{b_i}, \dots, b_n \rangle$  required in (1) cannot hold for all  $i = 1, \dots, n$ , and hence  $\mathcal{A}$  cannot be matched to  $\mathcal{B}$ . ■

With the notion of matched bases at hand, we now introduce that of matched  $K$ -subspaces of  $L$ .

**Definition 2.4** *Let  $A, B$  be  $n$ -dimensional  $K$ -subspaces in the field extension  $L$ . We say that  $A$  is matched to  $B$  if every basis  $\mathcal{A}$  of  $A$  can be matched to a basis  $\mathcal{B}$  of  $B$ .*

By the above lemma, if  $A$  is matched to  $B$ , then  $1 \notin B$ . Conversely, is the condition  $1 \notin B$  sufficient to guarantee that any subspace  $A$  of the same dimension as  $B$  is matched to  $B$ ? We shall see that the answer depends on properties of the field extension  $K \subset L$ .

**Definition 2.5** *Let  $K \subset L$  be a field extension. We say that  $L$  has the linear matching property if, for every  $n \geq 1$  and every  $n$ -dimensional subspaces  $A, B$  of  $L$  with  $1 \notin B$ , the subspace  $A$  is matched to  $B$ .*

We shall prove the following results in Section 5.

**Theorem 2.6** *Let  $K \subset L$  be a field extension, with  $K$  commutative and central in  $L$ . Then  $L$  has the linear matching property if and only if  $L$  contains no proper finite-dimensional extension over  $K$ .<sup>1</sup>*

**Corollary 2.7** *Let  $L$  be a commutative finite-dimensional Galois extension of the (commutative) field  $K$ . Then  $L$  has the linear matching property if and only if  $L$  is an extension of  $K$  of prime degree.*

In contrast, no special hypothesis on  $L$  is needed to guarantee that any  $n$ -dimensional subspace  $B$  avoiding  $1$  is matched to itself.

**Theorem 2.8** *Let  $K \subset L$  be a field extension, with  $K$  commutative and central in  $L$ . Let  $B$  be a finite-dimensional subspace of  $L$ . Then  $B$  is matched to itself if and only if  $1 \notin B$ .*

The proofs of these results involve delicate linearized versions, obtained in [4] and recalled in Section 4, of classical addition theorems due to Kemperman and Olson.

---

<sup>1</sup>Our original statement of Theorem 2.6 in the published version of this paper [Journal of Algebra 324 (2010) 3420-3430] was incorrect, as pointed out to us by Professors Akbari and Aliabadi. It mistakenly stated that the linear matching property was equivalent to  $L$  being either transcendental or an extension of prime degree over  $K$ , thereby missing all finite-dimensional extensions of non-prime degree having no proper intermediate extensions. (See Remark 5.4).

### 3 Dimension criteria for matchable bases

Let  $K \subset L$  be a field extension, with  $K$  commutative and central in  $L$ , and let  $A, B \subset L$  be  $n$ -dimensional  $K$ -subspaces of  $L$ . In this section, we reformulate the property of a basis  $\mathcal{A}$  of  $A$  to be matchable to some basis of  $B$ , in terms of suitable dimension estimates.

**Proposition 3.1** *Let  $\mathcal{A} = \{a_1, \dots, a_n\}$  be a basis of  $A$ . Then  $\mathcal{A}$  can be matched to a basis of  $B$  if and only if, for all  $J \subset \{1, \dots, n\}$ , we have*

$$\dim \bigcap_{i \in J} (a_i^{-1} A \cap B) \leq n - |J|. \quad (2)$$

For the proof of this equivalence in Section 3.2, we shall need a linear version of the classical marriage theorem of Hall [7].

#### 3.1 Free transversals

Let  $E$  be a vector space over the field  $K$  and let  $\mathcal{E} = \{E_1, E_2, \dots, E_n\}$  be a collection of vector subspaces of  $E$ . A *free transversal* for  $\mathcal{E}$  is a free family of vectors  $\{x_1, \dots, x_n\}$  in  $E$  satisfying  $x_i \in E_i$  for all  $i = 1, \dots, n$ . The following result of Rado [18] gives necessary and sufficient conditions for the existence of a free transversal for  $\mathcal{E}$ , very similar to those of Hall's marriage theorem. See also [13, 1, 14].

**Theorem 3.2** *Let  $E$  be a vector space over  $K$  and let  $\mathcal{E} = \{E_1, E_2, \dots, E_n\}$  be a family of vector subspaces of  $E$ . Then  $\mathcal{E}$  admits a free transversal if and only if*

$$\dim \sum_{i \in J} E_i \geq |J| \quad (3)$$

for all  $J \subset \{1, \dots, n\}$ .

It is not too difficult to prove this result directly, by properly mimicking a proof of its classical counterpart. In the above-mentioned paper of Rado, Theorem 3.2 arises as a particular case of a more general theorem concerning the existence of independent transversals in (possibly infinite) matroids. A finite version would read as follows [17, Chapter 12.2].

**Theorem 3.3** *Let  $F$  be a finite set, let  $\mathcal{F} = \{F_1, \dots, F_n\}$  be a family of subsets of  $F$ , and let  $M$  be a matroid over  $F$  with rank function  $r$ . Then the family  $\mathcal{F}$  admits a transversal which is independent in  $M$  if and only if one has*

$$r\left(\bigcup_{i \in J} F_i\right) \geq |J| \quad (4)$$

for all  $J \subset \{1, \dots, n\}$ .

Theorem 3.2 can be derived from Theorem 3.3 as follows. For each  $1 \leq i \leq n$ , pick a basis  $F_i$  of the subspace  $E_i$ , let  $\mathcal{F} = \{F_1, \dots, F_n\}$ , and set

$$F = \bigcup_{1 \leq i \leq n} F_i.$$

As matroid  $M$  over  $F$ , we consider the collection of linearly independent subsets in  $F$ , with rank function  $r$  defined by

$$r(S) = \dim_K \langle S \rangle$$

for all subsets  $S \subset F$ . Here, as earlier,  $\langle S \rangle$  denotes the subspace of  $E$  spanned by  $S$ . We now apply Theorem 3.3 in this situation. It is clear, from the definition of the rank function  $r$ , that

$$r\left(\bigcup_{i \in J} F_i\right) = \dim \bigoplus_{i \in J} E_i.$$

Thus, conditions (3) and (4) are equivalent, and an independent transversal for  $\mathcal{F}$  given by Theorem 3.3 yields a free transversal for the family  $\mathcal{E}$ .

## 3.2 Proof of Proposition 3.1

We shall use the following standard notation. We denote by

$$B^* = \{f : B \rightarrow K \mid f \text{ is linear}\}$$

the *dual* of  $B$ . Moreover, for any subspace  $C \subset B$ , we denote by

$$C^\perp = \{f \in B^* \mid C \subset \ker f\}$$

the *orthogonal* of  $C$  in  $B^*$ . Recall that  $\dim C^\perp = \dim B - \dim C$ .

We now prove Proposition 3.1, using Theorem 3.2 as a key ingredient.

**Proof.**  $\Rightarrow$ ) Assume first that  $\mathcal{A}$  is matched to the basis  $\mathcal{B} = \{b_1, \dots, b_n\}$  of  $B$ . It follows from condition (1) that

$$a_i^{-1}A \cap B \subset \langle b_1, \dots, \widehat{b_i}, \dots, b_n \rangle$$

for all  $1 \leq i \leq n$ . This implies, for any  $J \subset \{1, \dots, n\}$ , that

$$\bigcap_{i \in J} (a_i^{-1}A \cap B) \subset \bigcap_{i \in J} \langle b_1, \dots, \widehat{b_i}, \dots, b_n \rangle = \langle \mathcal{B} \setminus \{b_i \mid i \in J\} \rangle.$$

It follows that  $\dim \bigcap_{i \in J} (a_i^{-1}A \cap B) \leq n - |J|$ , as claimed.

$\Leftarrow$ ) Assume now that, for all  $J \subset \{1, \dots, n\}$ , we have

$$\dim \bigcap_{i \in J} (a_i^{-1}A \cap B) \leq n - |J|.$$

Taking the orthogonal in the dual space  $B^*$ , we get

$$\dim \left( \bigcap_{i \in J} (a_i^{-1}A \cap B) \right)^\perp \geq |J|,$$

and hence

$$\dim \sum_{i \in J} (a_i^{-1}A \cap B)^\perp \geq |J|.$$

By Theorem 3.2, the linear version of Hall's theorem, the above dimension bounds imply the existence of a free transversal

$$\varphi_1, \dots, \varphi_n \in B^*$$

for the system of subspaces  $\{(a_i^{-1}A \cap B)^\perp\}_{1 \leq i \leq n}$ . In other words, we have

$$\varphi_i \in (a_i^{-1}A \cap B)^\perp \tag{5}$$

for all  $1 \leq i \leq n$ , and  $\{\varphi_1, \dots, \varphi_n\}$  is free and hence a basis of  $B^*$ .

Let  $\mathcal{B} = \{b_1, \dots, b_n\}$  be the unique basis of  $B$  whose dual basis  $\mathcal{B}^*$  equals  $\{\varphi_1, \dots, \varphi_n\}$ , i.e. such that  $b_i^* = \varphi_i$  for all  $i$ . By (5), we have

$$b_i^* (a_i^{-1}A \cap B) = \{0\},$$

whence  $a_i^{-1}A \cap B \subset \langle b_1, \dots, \widehat{b_i}, \dots, b_n \rangle$  for all  $i$ , as desired. ■



## 4 Linear versions of some additive theorems

In order to exploit the equivalence given by Proposition 3.1, we shall need tools to establish the required dimension estimates (2). These tools will be conveniently provided by two results in linearized additive number theory, both established in [4].

Our first tool is a linear version of a classical theorem of Kemperman [11].

**Theorem 4.1** *Let  $K \subset L$  be a field extension, with  $K$  commutative and central in  $L$ . Let  $A, B$  be finite-dimensional  $K$ -subspaces of  $L$  such that  $K \subset A \cap B$ . Suppose there exist subspaces  $\overline{A}, \overline{B} \subset L$  such that*

$$A = K \oplus \overline{A}, \quad B = K \oplus \overline{B} \quad \text{and} \quad K \cap (\overline{A} + \overline{B} + \langle \overline{A}\overline{B} \rangle) = \{0\}.$$

*Then*

$$\dim \langle AB \rangle \geq \dim A + \dim B - 1.$$

For the proof of Theorem 2.8 in Section 5.1, we shall actually use the following corollary.

**Corollary 4.2** *Let  $U, V$  be finite-dimensional  $K$ -subspaces of  $L$ . Assume that  $U, V$  and  $UV$  are all three contained in a  $K$ -subspace  $X$  of  $L$  such that  $K \cap X = \{0\}$ . Then*

$$\dim X \geq \dim U + \dim V.$$

**Proof.** Let  $A = K \oplus U, B = K \oplus V$ . Then  $K \cap (U + V + \langle UV \rangle) = \{0\}$ . Therefore Theorem 4.1 applies, and gives

$$\dim \langle AB \rangle \geq \dim A + \dim B - 1.$$

Since  $\langle AB \rangle = K \oplus (U + V + \langle UV \rangle) \subset K \oplus X$ , this gives  $\dim \langle AB \rangle \leq \dim X + 1$ . With the equalities  $\dim A = \dim U + 1$  and  $\dim B = \dim V + 1$ , we then derive

$$\dim X \geq \dim \langle AB \rangle - 1 \geq \dim A + \dim B - 2 \geq \dim U + \dim V,$$

as desired. ■

Our second promised tool from [4] is a linear version of a classical theorem of Olson [16]. It will be used in the proof of Theorem 2.6 in Section 5.2.

**Theorem 4.3** *Let  $K \subset L$  be a field extension, with  $K$  commutative and central in  $L$ . Let  $A, B$  be finite-dimensional  $K$ -subspaces of  $L$  distinct from  $\{0\}$ . Then there exist a  $K$ -subspace  $S$  of  $\langle AB \rangle$  and a subfield  $M$  of  $L$  such that*

- (1)  $K \subset M \subset L$ ,
- (2)  $\dim S \geq \dim A + \dim B - \dim M$ ,
- (3)  $MS = S$  or  $SM = S$ .

## 5 Proofs of the main results

Let again  $K \subset L$  be a field extension, with  $K$  commutative and central in  $L$ . Let  $A, B$  be  $n$ -dimensional  $K$ -subspaces of  $L$ . The above linearized versions of additive theorems will allow us to fulfill, under appropriate circumstances, the dimension estimates required by Proposition 3.1, and thereby to prove Theorem 2.6 and 2.8.

### 5.1 Proof of Theorem 2.8

**Theorem 5.1** *Let  $B$  be a finite-dimensional  $K$ -subspace of  $L$ . Then  $B$  is matched to itself if and only if  $1 \notin B$ .*

**Proof.** We already know from Lemma 2.3 that if  $B$  contains 1, then  $B$  cannot be matched to itself. Conversely, assume  $1 \notin B$ . Let  $\mathcal{A} = \{a_1, \dots, a_n\}$  be any basis of  $B$ . For  $J \subset \{1, \dots, n\}$ , denote

$$V_J = \bigcap_{i \in J} (a_i^{-1}B \cap B) = \{x \in B \mid a_i x \in B \text{ for all } i \in J\}.$$

It follows from Proposition 3.1 that  $\mathcal{A}$  can be matched to another basis of  $B$  if and only if

$$\dim V_J \leq n - |J| \tag{6}$$

for all  $J \subset \{1, \dots, n\}$ . Denote now  $B_J$  the subspace of  $B$  spanned by the subset  $\{a_i \mid i \in J\}$  of  $\mathcal{A}$ . Then we have  $\dim B_J = |J|$ , and

$$B_J V_J \subset B$$

by construction. Since  $1 \notin B$ , Corollary 4.2 applies, with  $U, V, X$  standing for  $B_J, V_J, B$  respectively. This gives

$$\dim B_J + \dim V_J \leq \dim B,$$

i.e. exactly condition (6). By Proposition 3.1, the basis  $\mathcal{A}$  can be matched to another basis of  $B$ . Therefore, the space  $B$  is matched to itself. ■

## 5.2 Proof of Theorem 2.6

We now turn to the characterization of all field extensions satisfying the linear matching property.

**Theorem 5.2** *Let  $K \subset L$  be a field extension, with  $K$  commutative and central in  $L$ . Then  $L$  has the linear matching property if and only if  $L$  contains no proper finite-dimensional extension over  $K$ .*

**Proof.** Assume first that  $L$  is neither purely transcendental nor an extension of prime degree. Then there is an element  $a \in L$ , of finite degree  $n \geq 2$  over  $K$ , such that  $K(a) \subsetneq L$ . In particular, we have

$$K(a) = \langle 1, a, \dots, a^{n-1} \rangle.$$

Set  $A = K(a)$ . Let now  $x \in L \setminus K(a)$ , and set

$$B = \langle a, \dots, a^{n-1}, x \rangle.$$

We claim that  $A$  is not matched to  $B$ . Indeed, consider the basis  $\mathcal{A} = \{1, a, \dots, a^{n-1}\}$  of  $A$ . Since  $A = K(a)$  is a subfield of  $L$ , we have

$$a_i^{-1}A \cap B = A \cap B = \langle a, \dots, a^{n-1} \rangle$$

for all  $1 \leq i \leq n$ . Therefore, the condition  $\dim \bigcap_{i \in J} (a_i^{-1}A \cap B) \leq n - |J|$  of Proposition 3.1 does not hold for  $J = \{1, \dots, n\}$ , for instance. It follows that  $\mathcal{A}$  cannot be matched to a basis of  $B$ .

Conversely, assume that the only finite-dimensional subfields of  $L$  extending  $K$  are  $K$ , and  $L$  itself if it is finite-dimensional over  $K$ . The field  $L = K$  contains no proper intermediate extension and vacuously satisfies the linear

matching property. Assume now  $L \neq K$ . Let  $A, B$  be  $n$ -dimensional  $K$ -subspaces of  $L$  with  $1 \notin B$ . Let  $\mathcal{A} = \{a_1, \dots, a_n\}$  be any basis of  $A$ . For any  $J \subset \{1, \dots, n\}$ , denote

$$V_J = \bigcap_{i \in J} (a_i^{-1}A \cap B) = \{x \in B \mid a_i x \in A \text{ for all } i \in J\}.$$

By Proposition 3.1 again, we know that  $\mathcal{A}$  can be matched to a basis of  $B$  if and only if

$$\dim V_J \leq n - |J| \quad (7)$$

for all  $J \subset \{1, \dots, n\}$ . As earlier, denote  $A_J$  the subspace of  $A$  spanned by the subset  $\{a_i \mid i \in J\}$  of  $\mathcal{A}$ . Then we have  $\dim A_J = |J|$ , and

$$A_J V_J \subset A.$$

Set  $W_J = K \oplus V_J$ . We have  $\dim W_J = \dim V_J + 1$ , and still  $A_J W_J \subset A$  by construction. By Theorem 4.3, applied to the subspaces  $A_J$  and  $W_J$ , there is an intermediate field extension  $K \subset M \subset L$  and a subspace  $T \subset \langle A_J W_J \rangle$  such that

$$\dim \langle A_J W_J \rangle \geq \dim A_J + \dim W_J - \dim M, \quad (8)$$

and  $MT = T$  or  $TM = T$ . We cannot have  $M = L$ , for otherwise  $T = L$ ; but as  $T \subset A_J W_J \subset A$ , this would imply  $A = L = B$ , contradicting the hypothesis  $1 \notin B$ . It follows that  $M = K$ , and inequality (8) yields

$$\dim A \geq |J| + \dim V_J,$$

since  $\langle A_J W_J \rangle \subset A$ ,  $\dim W_J = \dim V_J + 1$  and  $\dim M = 1$ . Therefore conditions (7) are satisfied, implying that  $\mathcal{A}$  can be matched to a basis of  $B$ . It follows that  $L$  has the linear matching property. ■

**Corollary 5.3** *Let  $L$  be a commutative finite-dimensional Galois extension of the (commutative) field  $K$ . Then  $L$  has the linear matching property if and only if  $L$  is an extension of  $K$  of prime degree.*

**Proof.** Indeed, for a Galois extension of degree  $n$ , the intermediate extensions are in reversing bijection with the subgroups of the Galois group  $G$  of order  $n$ . Thus, if  $n$  is not a prime number, then  $G$  will have proper subgroups  $\{1\} \neq H \neq G$ , thereby yielding proper intermediate extensions  $L \supsetneq M \supsetneq K$ . ■

**Remark 5.4** For any non-prime integer  $n > 1$ , there exists a field extension  $K \subset L$  of characteristic 0 and degree  $n$  admitting no proper intermediate extension. It can be constructed as follows. Take  $L = k(X_1, \dots, X_n)$  the field of rational functions in the commutative variables  $X_1, \dots, X_n$  over an arbitrary field  $k$  of characteristic 0. Set  $S = L^{S_n}$  the subfield of  $L$  of rational symmetric functions. The field  $L$  can be regarded as the decomposition field of the polynomial

$$P(T) = \prod_{i=1}^n (T - X_i) \in S[T].$$

Therefore  $L$  is a normal extension of  $S$ . Since  $L$  is of characteristic 0, it is a Galois extension of  $S$ . Its Galois group is  $S_n$  so  $L$  has degree  $n!$  over  $S$ . The subgroup  $S_{n-1} \subset S_n$  is maximal. Therefore, if we set  $K = L^{S_{n-1}}$ , the invariant subfield under the group  $S_{n-1}$ , then  $L$  is an extension of  $K$  of degree  $n$  with no proper intermediate extension.

### 5.3 A refinement

Even if the extension  $K \subset L$  does not satisfy the linear matching property, it is still possible to match some subspaces  $A, B$  of  $L$  under suitable circumstances. Let  $n_0(K, L)$  denote the smallest degree of an intermediate field extension  $K \subsetneq M \subset L$ . Thus  $n_0(K, L) \geq 2$ , and  $n_0(K, L) = \infty$  if the extension is purely transcendental. Slightly adapting the proof of Theorem 2.6 yields the following result.

**Theorem 5.5** Let  $K \subset L$  be a field extension, with  $K$  commutative and central in  $L$ . Let  $A, B \subset L$  be  $n$ -dimensional subspaces of  $L$ , with  $1 \notin B$  and  $n < n_0(K, L)$ . Then  $A$  is matched to  $B$ .

**Proof.** Let  $\mathcal{A} = \{a_1, \dots, a_n\}$  be any basis of  $A$ . We proceed as in the proof of Theorem 2.6, and use the same notation  $V_J, A_J, W_J = K \oplus V_J$  for  $J \subset \{1, \dots, n\}$ . In order to ensure that  $\mathcal{A}$  can be matched to a basis of  $B$ , it suffices to check the condition

$$\dim V_J \leq n - |J| \tag{9}$$

for all  $J \subset \{1, \dots, n\}$ . We have  $A_J W_J \subset A$ . By Theorem 4.3 applied to  $A_J$  and  $W_J$ , there is an intermediate field extension  $K \subset M \subset L$  and a subspace  $T \subset \langle A_J W_J \rangle$  such that

$$\dim \langle A_J W_J \rangle \geq \dim A_J + \dim W_J - \dim M, \tag{10}$$

and  $MT = T$  or  $TM = T$ . This means that  $T$  is either a left or a right  $M$ -module, whence  $\dim M$  divides  $\dim T$ . But since  $T \subset \langle A_J W_J \rangle \subset A$ , it follows that  $\dim M \leq n$ . Now, our assumption  $n < n_0(K, L)$  implies  $M = K$ . Therefore, inequality (10) yields

$$\dim A \geq |J| + \dim V_J,$$

since  $\langle A_J W_J \rangle \subset A$ ,  $\dim A_J = |J|$ ,  $\dim W_J = \dim V_J + 1$  and  $\dim M = 1$ . Thus (9) is satisfied, implying that  $\mathcal{A}$  can be matched to a basis of  $B$ . ■

## 6 Strong matchings

Here we turn to a related, but much stronger notion of matching between subspaces. An existence criterion for such matchings is much easier to establish, as we do now, independently of the preceding results.

Let  $K \subset L$  be a field extension, and let  $A, B$  be finite-dimensional  $K$ -subspaces of  $L$  distinct from  $\{0\}$ .

**Definition 6.1** *A strong matching from  $A$  to  $B$  is a linear isomorphism  $\varphi : A \rightarrow B$  such that any basis  $\mathcal{A}$  of  $A$  is matched to the basis  $\varphi(\mathcal{A})$  of  $B$ , in the sense of Definition 2.1.*

We start with an easy equivalent reformulation of this notion, and then proceed with the promised existence criterion for strong matchings.

**Lemma 6.2** *Let  $\varphi : A \rightarrow B$  be an isomorphism of  $K$ -vector spaces. The following two statements are equivalent.*

1. *The map  $\varphi$  is a strong matching from  $A$  to  $B$ .*
2. *For any  $0 \neq a \in A$  and any subspace  $H \subset A$  such that  $A = \langle a \rangle \oplus H$ , we have  $a^{-1}A \cap B \subset \varphi(H)$ .*

**Proof.** Assume  $\varphi$  is a strong matching. Let  $0 \neq a \in A$ , and let  $H \subset A$  be any  $K$ -subspace such that  $A = \langle a \rangle \oplus H$ . Let  $\{a_2, \dots, a_n\}$  be any basis of  $H$ . Then  $\mathcal{A} = \{a, a_2, \dots, a_n\}$  is a basis of  $A$ . Hence  $\mathcal{A}$  is matched to  $\varphi(\mathcal{A}) = \{\varphi(a), \varphi(a_2), \dots, \varphi(a_n)\}$ . This implies that  $a^{-1}A \cap B$  is a subspace of  $\langle \varphi(a_2), \dots, \varphi(a_n) \rangle = \varphi(H)$ .

Conversely, assume statement 2 holds. Let  $\mathcal{A} = \{a_1, a_2, \dots, a_n\}$  be a basis of  $A$ . For any  $i = 1, \dots, n$ , set  $H_i = \langle a_1, \dots, \widehat{a_i}, \dots, a_n \rangle$ . Then we must have  $a_i^{-1}A \cap B \subset \langle \varphi(a_1), \dots, \widehat{\varphi(a_i)}, \dots, \varphi(a_n) \rangle$ . This proves that the basis  $\mathcal{A}$  is matched to  $\varphi(\mathcal{A})$ . Hence, the map  $\varphi$  is a strong matching from  $A$  to  $B$ . ■

**Theorem 6.3** *Let  $K \subset L$  be a field extension. Let  $A, B$  be  $n$ -dimensional  $K$ -subspaces of  $L$  distinct from  $\{0\}$ . There is a strong matching from  $A$  to  $B$  if and only if  $AB \cap A = \{0\}$ . In this case, any isomorphism  $\varphi : A \rightarrow B$  is a strong matching.*

**Proof.** Assume  $\varphi : A \rightarrow B$  is a strong matching. By Lemma 6.2, we obtain for any  $0 \neq a \in A$ :

$$a^{-1}A \cap B \subset \bigcap_H \varphi(H) = \varphi \left( \bigcap_H H \right),$$

where  $H$  ranges over all subspaces of  $A$  such that  $A = \langle a \rangle \oplus H$ . But of course, the intersection of all such subspaces  $H$  is reduced to  $\{0\}$ . Hence, we have  $a^{-1}A \cap B = \{0\}$  for any  $0 \neq a \in A$ . This means that  $AB \cap A = \{0\}$ .

Conversely, assume  $AB \cap A = \{0\}$ , and let  $\varphi : A \rightarrow B$  be any isomorphism. Then, for all  $0 \neq a \in A$ , we have  $a^{-1}A \cap B = \{0\}$ , whence  $a^{-1}A \cap B \subset \varphi(H)$  for any subspace  $H \subset A$ . It follows from Lemma 6.2 that  $\varphi$  is a strong matching from  $A$  to  $B$ , as claimed. ■

**Acknowledgement.** We are most grateful to Professors Akbari and Aliabadi for having pointed out to us the now corrected gap in our published version of Theorem 2.6.

## References

- [1] J. L. AROCHA, B. LLANO and M. TAKANE, *The theorem of Philip Hall for vector spaces*, An. Inst. Mat. Univ. Nac. Autónoma México **32** (1992), 1–8 (1993).
- [2] R. DIESTEL, *Graph Theory*, Graduate Text in Mathematics **173**, Springer-Verlag, New York, 1997.
- [3] S. ELIAHOU and C. LECOUVEY, *Matchings in arbitrary groups*, Adv. in Appl. Math. **40** (2008), 219–224.

- [4] S. ELIAHOU and C. LECOUEY, *On linear versions of some addition theorems*, Linear Multilinear Algebra **57** (2009), 759–775.
- [5] S. ELIAHOU, M. KERVAIRE and C. LECOUEY, *On the product of vector spaces in a commutative field extension*, J. Number Theory **129** (2009), 339–348.
- [6] C. K. FAN and J. LOSONCZY, *Matchings and canonical forms in symmetric tensors*, Adv. Math. **117** (1996), 228–238.
- [7] P. HALL, *On representatives of subsets*, J. London Math. Soc. **10** (1935), 26–30.
- [8] Y. O. HAMIDOUNE, *On Group bijections  $\phi$  with  $\phi(B) = A$  and  $\forall a \in B, a\phi(a) \notin A$* , preprint, arXiv:0812.2522v1 [math.CO].
- [9] X.D. HOU, *On a vector space analogue of Kneser’s theorem*, Linear Algebra Appl. **426** (2007), 214–227.
- [10] X. D. HOU, K. H. LEUNG AND Q. XIANG, *A generalization of an addition theorem of Kneser*, J. Number Theory **97** (2002), 1–9.
- [11] J. H. B. KEMPERMAN, *On complexes in a semigroup*, Indag. Math. **18** (1956), 247–254.
- [12] J. LOSONCZY, *On matchings in groups*, Adv. in Appl. Math. **20** (1998), 385–391.
- [13] L. MIRSKY and H. PERFECT, *Systems of representatives*, J. Math. Anal. Appl. **15** (1966), 520–568.
- [14] A. G. MOSHONKIN, *Concerning Hall’s theorem*, Mathematics in St.Petersburg, 73–77, Amer. Math. Soc. Transl. Ser. 2, **174**, Amer. Math. Soc., Providence, RI, 1996.
- [15] M. B. NATHANSON, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Graduate Text in Mathematics **165**, Springer-Verlag, New York, 1996.
- [16] J. E. OLSON, *On the sum of two sets in a group*, J. Number Theory **18** (1984), 110–120.



- [17] J. G. OXLEY, *Matroid theory*, Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1992.
- [18] R. RADO, *A theorem on independence relations*, Quart. J. Math., Oxford Ser. **13** (1942), 83–89.
- [19] E. K. WAKEFORD, *On canonical forms*, Proc. London Math. Soc. **18** (1918-1919), 403–410.